H

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,021	01/25/2001	Daisukc Suzuki	81942.0012	6351

26021 7590 06/14/2004

HOGAN & HARTSON L.L.P.
500 S. GRAND AVENUE
SUITE 1900
LOS ANGELES, CA 90071-2611

EXAMINER
COLIN, CARL G

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 06/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/771,021	**Applicant(s)** SUZUKI ET AL.	
	Examiner Carl Colin	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 January 2001* .

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 January 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) □ Interview Summary (PTO-413) Paper No(s). _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: .

DETAILED ACTION

1. Pursuant to USC 131, claims 1-19 are presented for examination.

Claim Objections

2. **Claim 17** is objected to because of the following informalities: in order to avoid rendering the claim indefinite, the term "capable of" should be corrected. Appropriate correction is required.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1, 5, 19, and the intervening claims are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claimed methods of claims 1 and 5 are not embodied in a computer hardware or software. The signal cited in claim 19 is not embodied in a computer hardware.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4.1 **Claims 1-2, 5-7, 11-13, and 16-19** are rejected under 35 U.S.C. 102(b) as being anticipated by "Masked Block Chaining Mode of Operation of a Block Cipher", January 1, 1997; IBM Technical Disclosure Bulletin, Volume 40, Issue Number 1, Pages 145-152.

4.2 **As per claims 1, 12, 17, 18, and 19, IBM TDB** discloses encryption method, comprising the steps of dividing a plaintext to be encrypted thereby to obtain a plaintext vector, for example (see section Simulation of Triple DES MBC) applying a predetermined transformation on the plaintext vector thereby to generate a transformation vector and generating a ciphertext by a product-sum operation between the components of a public key vector and the components of the plaintext vector and the transformation vector, for example (see section Simulation of Triple DES MBC see also Security Attributes at the beginning).

As per claim 2, IBM TDB discloses the limitation of wherein the product-sum operation with the components of the public key vector is performed using alternately a component of the plaintext vector and a component of the transformation vector, for example (see section Simulation of Triple DES MBC see also Security Attributes at the beginning).

Claim 13 is similar to the rejected **claims 1 and 2** except for incorporating the claimed method into a system. Therefore, **claim 13** is rejected on the same rationale as the rejection of **claims 1 and 2**.

As per claims 5 and 16, IBM TDB discloses an encryption method, comprising the step of generating a product-sum type ciphertext using a first vector depending on a plaintext and a second vector having components obtained by a modulo transformation of base products wherein the first vector is composed of a plaintext vector obtained by dividing a plaintext to be encrypted and a transformation vector obtained by a transformation of the plaintext vector using a predetermined function and. wherein the base product is obtained by both normal bases satisfying $b_i > m_{i-1}$ (bi is a base in the base product, m_{i-1} is a component of the first vector, i is an element of a subset S of a universal set U = { 2, 3, ..., K}, and K is the number of components of the first and second vector) :and reduced bases satisfying $b_j <= m_{j-1}$ (b_j is a base in the base product, m_{j-1} is a component of the first vector, and j is an element of a complementary set of the subset S), for example (see sections Simulation of Triple DES MBC and Objectives of Triple DES masked Block Chaining; see also Security Attributes at the beginning).

As per claims 6 and 7, IBM TDB discloses the limitation of, wherein the transformation vector is decrypted depending on decrypted components of the plaintext vector), for example (see sections Simulation of Triple DES MBC and Objectives of Triple DES masked Block Chaining).

As per claim 11, IBM TDB discloses the encryption method of claim 4, wherein a reduced-base part is decrypted depending on a decrypted normal-base part, for example (see sections Simulation of Triple DES MBC and Objectives of Triple DES masked Block Chaining).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.1 **Claims 3-4, 8-10, and 14-15** are rejected under 35 U.S.C. 103(a) as being unpatentable over "Masked Block Chaining Mode of Operation of a Block Cipher", January 1, 1997; IBM Technical Disclosure Bulletin, Volume 40, Issue Number 1, Pages 145-152 in view of Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone; Handbook of Applied Cryptography; 1997 by CRC Press LLC; Pages 185-186 and pages 228-233.

5.2 **As per claims 3-4 and 14-15, IBM TDB** substantially discloses the encryption method and system of claim 1, wherein: the components of the plaintext vector and the transformation vector are expressed by (m_1, m_2, ..., m_K); and as the bases bi, a normal base satisfying bi m_{i-1} is used when the m_{i-1} is a component of the plaintext vector while a reduced base satisfying bi c m_{i-1} is used when the m_{i-1} is a component of the transformation vector. **IBM TDB** further discloses using a Public key and using a base-product but does not explicitly mentioned that the key is obtained by a modulo transformation, which is obvious to one skilled in the art of cryptography. Therefore, the step of: the components of the public key vector are obtained by a modulo transformation of the components Bi of a base-product vector (B_1, B_2, ..., B_K) (where B_i = vi b_1 b_2 ... bi, with random numbers v_i and bases b_i (1<= i <=K)) is disclosed except the modulo part. A modulus key is also well known in the art of cryptography. **Menezes et al.** discloses components of the public key vector obtained by a modulo transformation of the components Bi of a base-product vector (B_1, B_2, ..., B_K) (where B_i = vi b_1 b_2 ... bi, with random numbers v_i and bases b_i (1<= i <=K)), for example (see pages 185-186). **Menezes et al.** further discloses that the modular multiplication may be slow depending on the hardware used but provides efficient security. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and system disclosed by IBM TDB to provide a modulo transformation of a base-product with random numbers as taught by **Menezes et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Menezes et al.** so as to provide efficient security.

As per claims 8 and 9, IBM TDB discloses the limitation of, wherein the transformation vector is decrypted depending on decrypted components of the plaintext vector), for example (see sections Simulation of Triple DES MBC and Objectives of Triple DES masked Block Chaining).

As per claim 10, IBM TDB discloses the encryption method of claim 4, wherein a reduced-base part is decrypted depending on a decrypted normal-base part, for example (see sections Simulation of Triple DES MBC and Objectives of Triple DES masked Block Chaining).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art block encoding and decoding dividing the message into a vector set before encryption. US Patent: 4,731,799 Longstaff et al.

6.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

CC

Carl Colin

Patent Examiner

June 9, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100